JOURNAL OF NUMBER THEORY 29, 21–30 (1988)

Abelian Extensions Generated by Division Points

D. S. DUMMIT

Department of Mathematics, University of Vermont, Burlington, Vermont 05405

AND

H. KISILEVSKY*

Department of Mathematics, Concordia University, Montreal, Quebec H3G 1M8

Communicated by W. Sinnott

Received March 15, 1987; revised August 27, 1987

1. INTRODUCTION

Let R be a commutative ring with identity (in the applications R will be a quotient of the integers $\mathbb{Z}$, the p-adic integers $\mathbb{Z}_p$, or an order $\mathcal{O}$ in an algebraic number field) and let A be an R-module. Let G be a profinite group acting continuously on the discrete group A and suppose that the actions of G and R on A commute. The cohomology groups $H^i(G, A)$ (continuous group cohomology) are naturally R-modules.

The group G acts on cochains via $a^\sigma(\cdots, \tau, \cdots) = \sigma a(\cdots, \sigma^{-1}\tau\sigma, \cdots)$, and it is known that the induced map on cohomology is the identity map, i.e., G acts trivially on $H^i(G, A)$. In particular, if σ is an element of the center $Z(G)$ of G then σ acts on $H^i(G, A)$ through its action on the coefficients.

PROPOSITION 1. *Let G be a profinite group acting continuously on the discrete R-module A as above. Suppose there exists a $\sigma \in Z(G)$ acting on A through a character χ_σ and let $\beta = \chi_\sigma(\sigma) - 1 \in R$. Then*

$$\beta \cdot H^i(G, A) = 0.$$

In particular $\mathfrak{b} \cdot H^i(G, A) = 0$ where $\mathfrak{b}$ is the ideal of R generated by the elements $\chi_\sigma(\sigma) - 1$ as σ runs over all elements in $Z(G)$ acting through a character χ_σ on A.

* Research supported in part by grants from NSERC and FCAR.

0022-314X/88 $3.00

Proof. $\beta \cdot H^i(G, A) = (\chi_\sigma(\sigma) - 1) \cdot H^i(G, A) = (\sigma - 1) \cdot H^i(G, A) = 0$, since σ acts on $H^i(G, A)$ through its action on A, i.e., through the character χ_σ and this action is trivial.

COROLLARY 1. *If G is a profinite abelian group acting continuously on the discrete R-module A through a character $\chi: G \to R^\times$ then $\mathfrak{b} \cdot H^i(G, A) = 0$ where $\mathfrak{b}$ is the ideal of R generated by the values $\chi(\sigma) - 1$ for $\sigma \in G$.*

Suppose now that G is abelian and that A is a cyclic torsion R-module. By choosing a generator x for A we may identify A with $R/\mathfrak{a}$ for some non-zero ideal $\mathfrak{a}$ of R. Then G acts on A by a character $\chi: G \to (R/\mathfrak{a})^\times$ defined by $\sigma x = \chi(\sigma)x$. Let $\mathfrak{b}$ be the ideal in R containing $\mathfrak{a}$ such that $\mathfrak{b}/\mathfrak{a}$ is the ideal generated by the values $\chi(\sigma) - 1$ in $R/\mathfrak{a}$ for $\sigma \in G$. Then by the corollary above, $\mathfrak{b} \cdot H^i(G, A) = 0$.

Let A^G denote the fixed points of A under G. Then

$$\begin{aligned} a \in A^G &\Leftrightarrow (\sigma - 1)\, a = 0 \qquad \text{for all} \quad \sigma \in G \\ &\Leftrightarrow (\chi(\sigma) - 1)\, a = 0 \qquad \text{for all} \quad \sigma \in G \\ &\Leftrightarrow \mathfrak{b} \cdot a = 0. \end{aligned}$$

Hence $A^G = \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ where $\mathfrak{b}^{-1}\mathfrak{a}$ denotes $\{x \in R \mid \mathfrak{b}x \subseteq \mathfrak{a}\}$ (usually denoted $[\mathfrak{a}:\mathfrak{b}]$).

If R is a Dedekind domain, then it is easy to conclude that

$$\beta \in \mathfrak{b} \Leftrightarrow \beta \cdot A^G = 0,$$

i.e., that $\mathfrak{b}$ is precisely the annihilator of A^G. In particular, it follows that $\operatorname{ann}(A^G) \cdot H^i(G, A) = 0$. Since cohomology commutes with direct sums, we obtain

THEOREM 1. *Let R be a Dedekind domain and let G be a profinite abelian group acting continuously on the discrete R-module A as above. Suppose that A is the direct sum of cyclic R-modules and that G acts on each summand of A. Let $\mathfrak{b} = \operatorname{ann}(A^G)$ be the annihilator in R of the fixed points A^G of A under G. Then*

$$\mathfrak{b} \cdot H^i(G, A) = 0 \qquad \text{for all} \quad i \geqslant 0.$$

This result gives a particularly simple annihilator for the cohomology groups in the applications below.

Remark. In general, let $\mathfrak{c}$ denote the ideal $[\mathfrak{a}: [\mathfrak{a}:\mathfrak{b}]]$ (so that $\mathfrak{c}/\mathfrak{a}$ is the "double annihilator" of $\mathfrak{b}/\mathfrak{a}$ in the quotient $R/\mathfrak{a}$), so that $\mathfrak{c}$ is the annihilator of A^G by the argument above. Then $\mathfrak{b} \subseteq \mathfrak{c}$ and the containment can be

proper if R is not Dedekind, so that the annihilator of A^G may not annihilate the cohomology groups. For example, take $R = \mathbb{Z}[2\sqrt{-2}]$, $\mathfrak{b} = (2, 4\sqrt{-2})$, and $\mathfrak{a} = (4, 4\sqrt{-2})$ (then $\mathfrak{b}$ is contained in the maximal ideal $\mathfrak{m} = (2, 2\sqrt{-2})$ and $\mathfrak{a}$ is the square of this maximal ideal). Then $[\mathfrak{a}:\mathfrak{b}] = \mathfrak{m}$ and so the double annihilator is $[\mathfrak{m}:\mathfrak{m}^2] = \mathfrak{m}$, which properly contains $\mathfrak{b}$. (We are indebted to R. Foote for this example.)

If R is an order in an algebraic number field with conductor $\mathfrak{f}$, then it is easy to see that $\mathfrak{b}$ and the ideal $\mathfrak{c} = [\mathfrak{a}: [\mathfrak{a}:\mathfrak{b}]]$ satisfy

$$\mathfrak{f}^2\mathfrak{c} \subseteq \mathfrak{b} \subseteq \mathfrak{c}$$

independent of the ideal $\mathfrak{a}$.

Define the abelian group A to be *rank one* if A is isomorphic to a subgroup of $\mathbb{Q}/\mathbb{Z}$. Then in the particularly simple case where $R = \mathbb{Z}$ we obtain

COROLLARY 2. *Let G be an abelian profinite group acting continuously on the discrete G-module A. Suppose that A is a direct sum of rank one groups and that G acts on each summand of A. If the exponent m of the fixed points A^G of A under G is finite, then*

$$m \cdot H^i(G, A) = 0.$$

In particular, if A is rank one and A^G is finite, then

$$|A^G| \cdot H^i(G, A) = 0.$$

Proof. We have

$$H^i(G, A) = \varinjlim H^i(G/H, A^H),$$

where the direct limit is taken over the open subgroups H of G. If $A = \sum A_j$ is the direct sum of rank one G-modules A_j, then $A^H = \sum A_j^H$ is the direct sum of the rank one G/H-modules A_j^H. The exponent m of A^G is also the exponent of $(A^H)^{G/H}$, the fixed points under G/H of A^H and by Theorem 1, $m \cdot H^i(G/H, A_j^H) = 0$, hence also $m \cdot H^i(G, A) = 0$.

2. APPLICATION TO TORSION IN MULTIPLICATIVE GROUPS AND TO ELLIPTIC CURVES

2.1. *A Theorem of Schinzel*

The first application is to a result[1] dealing with the abelian extensions of a field F generated by mth roots of elements of the multiplicative group $F^\times$

[1] Which occurs as an exercise in Tate "Les Conjectures de Stark sur les Fonctions L'Artin en $s = 0$," p. 85, where, as Tate says, the result "semble être du à A. Schinzel... ."

of F. Let F be a field and let K be a Galois extension of F with Galois group G. Let $\mu(K)$ (resp. $\mu(F)$) denote the roots of unity in K (resp. F). Define

$$\tilde{K} = K^\times/\mu(K)$$
$$\tilde{F} = F^\times/\mu(F).$$

There is a natural exact sequence of G-modules

$$1 \to \mu(K) \to K^\times \to \tilde{K} \to 1. \tag{2}$$

Taking cohomology we obtain the exact sequence

$$1 \to \mu(F) \to F^\times \to (\tilde{K})^G \to H^1(G, \mu(K)) \to 1$$

since $H^1(G, K^\times) = 0$. This gives

$$1 \to \tilde{F} \to \tilde{K}^G \to H^1(G, \mu(K)) \to 1$$

so that

$$\tilde{K}^G/\tilde{F} \cong H^1(G, \mu(K)). \tag{3}$$

Now, if $\alpha \in K^\times$ and $\tilde{\alpha}$ is the image of α in $\tilde{K}$, then

$$\begin{aligned} \tilde{\alpha} \in \tilde{K}^G &\Leftrightarrow \frac{\sigma(\alpha)}{\alpha} \in \mu(K) \qquad \text{for all } \sigma \in G \\ &\Leftrightarrow \left(\frac{\sigma(\alpha)}{\alpha}\right)^m = 1 \qquad \text{for some } m \text{ and for all } \sigma \in G \\ &\Leftrightarrow \alpha^m \in F \end{aligned}$$

By Corollary 2, if G is an abelian group, then the cohomology group in (3) is annihilated by $|\mu(F)|$ if $|\mu(F)| < +\infty$ since these are the fixed points of $\mu(K)$ under G.

Letting $K = F^{ab}$, the maximal abelian extension of F, we see that if α generates an abelian extension of F and $\alpha^m \in F^\times$ for some m then, up to a root of unity, $\alpha^{|\mu(F)|} \in F^\times$. The argument above shows more precisely that $\alpha^e \in F^\times$, where $e = |\mu_m(F)|$ is the number of mth roots of unity in F.

This result shows that, up to roots of unity, the only abelian root extensions of F are the Kummer extensions of F. In this form, the result appears in Schinzel [S] as Theorem 2.

This can be rephrased in terms of the torsion in the abelian group $(F^{ab})^\times/F^\times$ (or in terms of the torsion in $K^\times/F^\times$ for any finite abelian extension K of F). We have the exact sequence

$$0 \to \mu(F^{ab})\, F^\times/F^\times \to (F^{ab\times}/F^\times)_{\text{tors}} \to (F^{ab\times}/\mu(F^{ab})\, F^\times)_{\text{tors}} \to 0,$$

where the term on the right is $(\tilde{F}^{ab}/\tilde{F})_{tors}$ by the computation following Eq. (3). Also, by the results above, this term is isomorphic to $\tilde{F}/\tilde{F}^n$ where $n = |\mu(F)|$. Explicitly: if $\beta \in F^{ab\times}$ represents a class in $(F^{ab\times}/\mu(F^{ab})\,F^\times)_{tors}$, then β differs by a root of unity from an element α with $\alpha^n \in F$. Then the isomorphism is given by mapping the class of β to the class of α^n in $\tilde{F}/\tilde{F}^n$. This gives the sequence

$$0 \to \mu(F^{ab})/\mu(F) \to (F^{ab\times}/F^\times)_{tors} \to \tilde{F}/\tilde{F}^n \to 0 \tag{4}$$

which describes the structure of the group $(F^{ab\times}/F^\times)_{tors}$. In particular, since $\mu(F^{ab})/\mu(F)$ is a divisible group, the sequence splits as abelian groups, which shows that

$$(F^{ab\times}/F^\times)_{tors} \cong \mu(F^{ab})/\mu(F) \oplus \tilde{F}/\tilde{F}^n \tag{5}$$

as abelian groups (but not as Galois modules) where $n = |\mu(F)|$, a direct sum of a divisible group and an infinite group of exponent dividing n. Similarly, for any *finite* abelian extension K of F, the torsion in $K^\times/F^\times$ is isomorphic to $\mu(K)/\mu(F)$ and a (finite) group of exponent at most $|\mu(F)|$ bounded independently of the abelian extension K. Note that the torsion in this quotient is *not* bounded as K runs over all Galois (not necessarily abelian) extension of F.

2.2. *Elliptic Curves with Complex Multiplication*

We now consider the analogous question of the abelian extensions generated by division of rational points on elliptic curves. Let E be an elliptic curve defined over the field F whose group of F-rational torsion is finite and let K be a Galois extension of F with Galois group G. We assume that E has *CM* by the maximal order $\mathcal{O}$ of the imaginary quadratic field k ($k \subseteq F$) so that the torsion points on E generate abelian extensions of F. Let $\bar{F}$ be a (fixed) algebraic closure of F.

For $\alpha \in \mathcal{O}$, let $[\alpha]$ denote multiplication by α on the elliptic curve and denote by E_α the kernel of multiplication by α and by $E(K)_{tors}$ the K-rational torsion points of E. Analogous to the exact sequence (2) we define $\tilde{E}(K)$ by the exact sequence

$$1 \to E(K)_{tors} \to E(K) \to \tilde{E}(K) \to 1 \tag{6}$$

which gives the exact sequence

$$1 \to E(F)_{tors} \to E(F) \to \tilde{E}(K)^G \to H^1(G, E(K)_{tors}) \to \cdots$$

so that

$$(\tilde{E}(K))^G/\tilde{E}(F) \cong \text{subgroup of } H^1(G, E(K)_{tors}). \tag{7}$$

Now, $\tilde{Q} \in (\tilde{E}(K))^G$ if and only if $Q^\sigma = Q$ up to an element of $E(K)_{tors}$, say $Q^\sigma = Q + Q'$ where Q' is an α-torsion element in $E(K)$ for some α. Then

$(\alpha Q)^\sigma = \alpha Q$ for all $\sigma \in G$ so that $\alpha Q = P \in E(F)$. Hence Q represents a torsion element in $(\tilde{E}(K)/\tilde{E}(F))$. Conversely, if Q represents a torsion element in this quotient, then $[\alpha]\, Q = P' + Q_\beta$ where $P' \in E(F)$ and Q_β is a β-torsion element of $E(K)$ for some β. Then $[\alpha\beta]\, Q = [\beta]\, P' = P \in E(F)$, so $Q^\sigma = Q$ modulo an $\alpha\beta$-torsion point, hence Q represents an element in $(\tilde{E}(K))^G/\tilde{E}(F)$. This shows that

$$(\tilde{E}(K))^G/\tilde{E}(F) \cong (\tilde{E}(K)/\tilde{E}(F))_{\text{tors}}. \tag{8}$$

Since $\mathcal{O}$ is the maximal order, $E_\alpha(\bar{F})$ is a cyclic $\mathcal{O}$-module for any $\alpha \in \mathcal{O}$, as follows: For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the Tate module $T_\mathfrak{p} = \varprojlim E_{\mathfrak{p}^n}$ of the $\mathfrak{p}^n$ division points on E is a rank one module over the completion $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}$ at $\mathfrak{p}$, hence free. It follows that $E_{\mathfrak{p}^n} \cong \mathcal{O}/\mathfrak{p}^n$ as $\mathcal{O}$-modules for any n, and hence $E_\alpha(\bar{F}) \cong \mathcal{O}/(\alpha)$ as $\mathcal{O}$-modules.

For any field K containing F, $E_\alpha(K)$ is an $\mathcal{O}$-submodule of $E_\alpha(\bar{F})$, hence is also a cyclic $\mathcal{O}$-module because $\mathcal{O}$ is a Dedekind domain. In particular, it follows that $E_\alpha(K) = E_\mathfrak{c}(\, = E_\mathfrak{c}(\bar{F}))$ where $\mathfrak{c} = \text{ann}(E_\alpha(K))$ and that for K/F finite, $E(K)_{\text{tors}}$ is a cyclic $\mathcal{O}$-module.

Assume now that $K = F(Q)$ is *abelian* over F. Let $\mathfrak{n}$ denote the annihilator in $\mathcal{O}$ of $E(F)_{\text{tors}}$. Then the cohomology group $H^1(G, E(K)_{\text{tors}})$ is annihilated by $\mathfrak{n}$ by Theorem 1. Hence by (7) and (8), the ideal $\mathfrak{n}$ annihilates $(\tilde{E}(K)/\tilde{E}(F))_{\text{tors}}$. This is the analogue of Schinzel's Theorem above and shows that, up to torsion points on E, the only abelian extensions of F generated by divisions of rational points in $E(F)$ are the "Kummer extensions." More precisely, if the point $Q' \in E(\bar{F})$ is the α-division of a point in $E(F)$ (i.e., $[\alpha]\, Q' \in E(F)$) which generates an abelian extension of F, then up to a torsion point (in $E(F^{\text{ab}})$), $Q' \equiv Q$ where $\mathfrak{e} \cdot Q \in E(F)$. Here $\mathfrak{e} = \text{g.c.d.}((\alpha), \mathfrak{n})$. Since

$$E_\mathfrak{e} = E_\alpha \cap E_\mathfrak{n} = E_\alpha \cap E(F) = E_\alpha(F)$$

we see that $\mathfrak{e}$ is the annihilator of $E_\alpha(F)$ and that the $\mathfrak{e}$ division points on E are all rational over F, so that Q generates a "Kummer extension" of F.

As before, this can be phrased in terms of the torsion in the quotient $E(F^{\text{ab}})/E(F)$: by definition, we have the exact sequence

$$0 \to E(F^{\text{ab}})_{\text{tors}} E(F)/E(F) \to (E(F^{\text{ab}})/E(F) \to \tilde{E}(F^{\text{ab}})/\tilde{E}(F) \to 0.$$

Taking the torsion in this sequence gives the exact sequence

$$0 \to E(F^{\text{ab}})_{\text{tors}} E(F)/E(F) \to (E(F^{\text{ab}})/E(F))_{\text{tors}} \to (\tilde{E}(F^{\text{ab}})/\tilde{E}(F))_{\text{tors}} \to 0$$

(in general, the exact sequence $0 \to A \to B \to C \to 0$ gives the exact sequence $0 \to A_{\text{tors}} \to B_{\text{tors}} \to C_{\text{tors}} \to 0$ if $A \subseteq B_{\text{tors}}$). Hence we have

$$0 \to E(F^{\text{ab}})_{\text{tors}}/E(F)_{\text{tors}} \to (E(F^{\text{ab}})/E(F))_{\text{tors}} \to (\tilde{E}(F^{\text{ab}})/\tilde{E}(F))_{\text{tors}} \to 0, \tag{9}$$

where the group on the right is the subgroup of $H^1(G, E_{\text{tors}})$ annihilated by n considered above. This sequence splits as abelian groups since the group on the left is divisible. Note that in this case the group on the right is *finite* since $E(F)$ is finitely generated and the quotient has finite exponent, so that in this case $(E(F^{\text{ab}})/E(F)_{\text{tors}}$ is the direct sum of a divisible group and a finite group.

Remark 1. If E has CM by a non-maximal order of conductor $\mathfrak{f}$ then $(E(F^{\text{ab}})/E(F))_{\text{tors}}$ is again the direct sum of $E(F^{\text{ab}})_{\text{tors}}/E(F)_{\text{tors}}$ with a finite group. This follows by considering an isogenous curve E' with CM by the maximal order. In this case, however, it is not as clear how the annihilator of the finite group is related to $E(F)$.

Remark 2. The results above are clearly valid for any abelian variety with complex multiplication.

3. Towers of Abelian Extensions

The fact that the exponent of the torsion in quotients of the type considered above is bounded over all abelian extensions has implications for towers of abelian extensions.

Let L/F be a Galois extension and let $A(L)$ be an abelian group which is a module for $\text{Gal}(L/F)$ such that $A(K) = A(L)^{\text{Gal}(L/K)}$ for every finite extension K of F contained in L.

Suppose that $A(L)$ is an $\mathcal{O}$-module for some Dedekind domain $\mathcal{O}$. Define $\tilde{A}$ by the exact sequence

$$0 \to A(K)_{\text{tors}} \to A(K) \to \tilde{A}(K) \to 0.$$

Then for K/F $(F \subseteq K \subseteq L)$ Galois with Galois group G we have

$$\tilde{A}(K)^G/\tilde{A}(F) \cong (\tilde{A}(K)/\tilde{A}(F))_{\text{tors}} \subsetneq H^1(G, A(K)_{\text{tors}}).$$

If G is abelian and $A(K)_{\text{tors}}$ is a direct sum of cyclic $\mathcal{O}$-modules on each of which G acts, then Theorem 1 shows that $H^1(G, A(K)_{\text{tors}})$ is annihilated by $\mathfrak{b} = \text{ann}(A(F)_{\text{tors}})$.

Suppose that $F \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq L$ is a tower of fields with K_i/F finite and Galois. Then for each i we have the sequence

$$0 \to A(K_i)_{\text{tors}} \to A(K_i) \to \tilde{A}(K_i) \to 0$$

and for $i \leqslant j$, $\tilde{A}(K_i) \subsetneq \tilde{A}(K_j)$.

Suppose now in addition that $K = \bigcup K_i$ is an abelian extension of F and that for each i, $A(K_i)_{\text{tors}}$ is a direct sum of cyclic $\mathcal{O}$-modules as above and that $\tilde{A}(K_i)$ is a finitely generated $\mathcal{O}$-module of rank r_i (so $r_i \leqslant r_j$ if $i \leqslant j$).

PROPOSITION 2. *If the ranks r_i are bounded, then there exists i_0 such that for all $i \geqslant i_0$,*

$$\tilde{A}(K_i) = \tilde{A}(K_{i_0}).$$

Proof. Suppose $r_i \leqslant r$ and $r_i = r$ for $i \geqslant i_1$. Then rank $\tilde{A}(K_i) = r$ for all $i \geqslant i_1$ and $\tilde{A}(K) = \bigcup \tilde{A}(K_i)$. Let $F = K_{i_1}$. Then

$$0 \to \tilde{A}(K_i)/\tilde{A}(F) \to \tilde{A}(K_j)/\tilde{A}(F) \to \tilde{A}(K_j)/\tilde{A}(K_i) \to 0$$

is a sequence of torsion modules for all $i, j \geqslant i_1$, and

$$\operatorname{ann}(\tilde{A}(K_i)/\tilde{A}(F)) = \mathfrak{b}_i \supseteq \mathfrak{b} = \operatorname{ann}(A(F)_{\text{tors}}) \qquad \text{for all } i,$$

so that each $\tilde{A}(K_i)/\tilde{A}(F)$ is a quotient of $(\mathcal{O}/\mathfrak{b})^r$.

For an $\mathcal{O}$-module M having a finite composition series $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_k = 0$ with $M_{i-1}/M_i \cong \mathcal{O}/\mathfrak{p}_i$ for $\mathfrak{p}_i \subset \mathcal{O}$ prime, define $\operatorname{Norm}_{\mathcal{O}}(M) = \prod_{i=1}^{k} \mathfrak{p}_i$. Then $N_i = \operatorname{Norm}_{\mathcal{O}}(\tilde{A}(K_i)/\tilde{A}(F))$ is a divisor of $\mathfrak{b}^r$ for all i. Let i_0 be such that N_{i_0} is the smallest ideal of $\mathcal{O}$ in $\{N_i\}$. (Equivalently, the corresponding module is one of minimal length as an $\mathcal{O}$-module.) Then for this choice of i_0 we clearly have $\tilde{A}(K_i) = \tilde{A}(K_{i_0})$ for all $i \geqslant i_0$.

3.1. *Application to Class Groups in $\hat{\mathbb{Z}}$-extensions*

Let F be a *CM* field with maximal real subfield F^+ and let K be an abelian *CM* extension of F (so K^+/F^+ is also abelian). Suppose S^+ is a finite set of primes $\{\mathfrak{p}_1^+, \ldots, \mathfrak{p}_n^+\}$ of F^+ none of which is infinitely decomposed in K^+ and such that each $\mathfrak{p}_i^+$ splits in F: $\mathfrak{p}_i^+ = \mathfrak{p}_i\bar{\mathfrak{p}}_i$. For any finite subextension L, $F \subseteq L \subseteq K$, let $I_S(L)$ be the group of fractional ideals of L supported at the primes in S. For each i, let $\mathfrak{P}_i$ be a prime of L dividing $\mathfrak{p}_i$ and let $I_S^-(L)$ be the subgroup of $I_S(L)$ generated by the ideals $\mathfrak{P}_i/\bar{\mathfrak{P}}_i$. Then

$$I_S^-(L)^{\operatorname{Gal}(L/F)}/I_S^-(F) \cong \sum_{i=1}^{n} \mathbb{Z}/e_i\mathbb{Z}, \tag{10}$$

where $e_i = e_i(L/F)$ is the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}_i$.

Denote by $P_S(L) \subseteq I_S(L)$ the subgroup of principal ideals in $I_S(L)$ and set $P_S^-(L) = P_S(L) \cap I_S^-(L)$. We have the exact sequence

$$0 \to E(L) \to E_S(L) \to P_S(L) \to 0,$$

where $E(L)$ is the group of units of L and $E_S(L) = \{\alpha \in L^\times \mid (\alpha) \in P_S(L)\}$ is the group of "S-units" of L. This induces the exact sequence

$$0 \to \mu(L) \to E_S^-(L) \to P_S^-(L)$$

on taking minus parts with respect to complex conjugation.

If $(\alpha) \in P_S^-(L)$, then $\alpha \in L^\times$ and $\alpha\bar{\alpha} = \varepsilon \in E(L)$. Since $\alpha\bar{\alpha} \in L^+$, $\varepsilon \in E(L^+)$, so that $\alpha^2\bar{\alpha}^2 = \varepsilon^2 = \varepsilon\bar{\varepsilon}$. Hence $\alpha^2/\varepsilon \in E_S^-(L)$ is a minus S-unit, so $(\alpha)^2 = (\alpha^2/\varepsilon) \in \text{Image}(E_S^-(L))$. This shows that

$$[P_S^-(L)]^2 \subseteq \text{Image}(E_S^-(L)) \subseteq P_S^-(L).$$

Letting $A(L) = E_S^-(L)$ above and noting that no prime of S is infinitely decomposed in K we see that the ranks of the groups $E_S^-(L)$ remain bounded as L varies over the finite subextensions of F, $F \subseteq L \subseteq K$, and so by Proposition 2, the groups $\tilde{A}(L) = E_S^-(L)/\mu(L)$ eventually stabilize. Since $[P_S^-(L)]^2 \subseteq \tilde{A}(L) \subseteq P_S^-(L)$ are free groups of equal rank, it follows that the groups $P_S^-(L)$ also eventually stabilize. Hence, for L sufficiently large and $F \subseteq L \subseteq L' \subseteq K$ we have

$$0 \to I_S^-(L)/P_S^-(L) \to I_S^-(L')^{\text{Gal}(L'/L)}/P_S^-(L') \to I_S^-(L')^{\text{Gal}(L'/L)}/I_S^-(L) \to 0$$

with $P_S^-(L) = P_S^-(L')$.

If $C_S^-(L')$ denotes the minus part of the class group of L' generated by the primes in S, then this sequence and (10) shows that $C_S^-(L')$ contains a subgroup isomorphic to

$$\sum_{\mathfrak{p}} \mathbb{Z}/e_{\mathfrak{p}}\mathbb{Z},$$

where the sum is taken over the primes of L in S and $e_{\mathfrak{p}}$ is the ramification index of such primes for L'/L.

If, for example, we take K/F to be a cyclotomic $\mathbb{Z}_p$ extension and S to be the set of primes of F dividing p, this shows that $C^-(K)$, the minus part of the class group of K, contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^s$ where s is the number of primes over p in F^+ which split in F, a well-known result of Iwasawa [I, Sect. 11.7].

Let $\mathbb{Q}_\infty$ be the (cyclotomic) $\hat{\mathbb{Z}}$-extension of $\mathbb{Q}$, i.e., $\mathbb{Q}_\infty$ is the composite of all the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ for all primes p. Denote by $\mathbb{Q}^n$ the unique subfield of $\mathbb{Q}_\infty$ of degree n over $\mathbb{Q}$. Let now K be the cyclotomic $\hat{\mathbb{Z}}$-extension of the CM field F: $K = F \cdot \mathbb{Q}_\infty$. Let N be an integer and choose a prime p which splits completely in $F\mathbb{Q}^N$. Let K_p be the $\mathbb{Z}_p$-extension of $F\mathbb{Q}^N$ contained in K. By the argument above we see that the group $C^-(K_p)$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^N$ and since K/K_p is a prime to p extension, it follows that $C^-(K_p)$ injects into $C^-(K)$ and so $C^-(K)$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^N$. It follows that $C^-(K)$ has p-primary subgroups whose ranks are unbounded as p varies, a result observed by Greenberg.

(It is likely, but unproven, that for each prime p the p-primary subgroup of $C^-(K)$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^\infty$. This would follow from the following: Given a prime p, find primes l such that

$p^{l-1} \equiv 1 \bmod l^2$. For such l, p splits in $\mathbb{Q}^l$ and if in addition the primes over p are split in F/F^+, then by the above argument we see that $C^-(K)$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^l$. Were there infinitely many such primes l, it would follow that $(\mathbb{Q}_p/\mathbb{Z}_p)^\infty \subseteq C^-(K)$.)

3.2. *Application to Points on Elliptic Curves over Certain $\mathbb{Z}_p$-extensions*

As a final application, we consider the ranks of *CM* elliptic curves in $\mathbb{Z}_p$-extensions. Let E be an elliptic curve defined over a field L having *CM* by the field k ($k \subseteq L$) and suppose that $L(E_{\text{tors}})$ is an abelian extension of k (for example, if E is defined over k). Let p be a prime and let K/k be a $\mathbb{Z}_p$-extension. Then R. Greenberg has shown that if K is not the anticyclotomic $\mathbb{Z}_p$-extension of k, then the rank of the Mordell-Weil group of E over the field LK is finite. In particular, the ranks of $E(L_i)$ are bounded ($L = L_0 \subseteq L_1 \subseteq \cdots \subseteq LK$). It follows from the above that in this situation

$$E(L_i)/E(L_i)_{\text{tors}} = E(L_{i_0})/E(L_{i_0})_{\text{tors}} \qquad \text{for all} \quad i \geqslant i_0$$

for some i_0, so that, modulo torsion, the Mordell-Weil groups stabilize up the tower. A similar result appears in Mazur [M, Proposition 6.11] with the additional assumption that the torsion in LK is finite.

References

[G] R. Greenberg, to appear.

[I] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math.* (2) **98** (1973), 246–326.

[M] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.

[S] A. Schinzel, Abelian binomials, power residues and exponential congruences, *Acta Arith.* **32** (1977), 245–274.